## OVERVIEW

This policy addresses the appropriate use and disclosure of information contained within the criminal history records as obtained from the Law Enforcement Information network (LEIN). It incorporates the regulations, policies and laws from the Michigan Department of Health and Human Services (MDHHS), Michigan State Police (MSP), Adam Walsh Act, Criminal Justice Information Services (CJIS) Policy Council Act, CJIS Security Policy, and CJIS addendum.

## LEGAL BASE

### Federal

28 CFR 20 provides provisions for criminal justice information (CJI) systems, dissemination, certification and penalties for misuse.

34 USC 20961 grants the MDHHS access to NCIC and NCIC III for investigated cases of child abuse, neglect or exploitation.

CJIS Security Policy provides guidelines and requirements for criminal justice agencies (CJA) to protect the CJI, both at rest and in transit. This includes transmission, dissemination and destruction of CJI.

### State

The Criminal Justice Information Services (CJIS) Policy Council Act, 1974 PA 163, as amended, MCL 28.214 provides MDHHS access to LEIN and fingerprint identification systems for the enforcement of child support laws and child and vulnerable adult protection laws.

Executive Order 1990-10 provides provisions for dissemination of criminal history record information to the Department of Social Services.

Social Welfare Act, 1939 PA 280, as amended, MCL 400.43b established the Office of Inspector General (OIG) as a criminal justice department under MDHHS.

### MSP Policy

CJIS Michigan Addendum is an adopted revision to the Michigan CJIS Security Policy that requires Michigan users to adhere to requirements in the FBI CJIS Security Policy, versions 5.1 and future.

MSP LEIN Policy Manual provides policy topics and rules on LEIN use.

Admin/ Court Rule

CJIS Administrative Rules (State Office of Administrative Hearings and Rules, Administrative Code: R 28.5101 - R 28.5414) provides general provisions, access, eligibility, and data dissemination provisions, NCIC access; authorized agencies, audit information and dissemination, and records.

Inter-Agency Contracts and Agreements

Signed contractual agreements between the Michigan State Police and the CJIS-0001, MDHHS/CSA. LEIN Memorandum of Agreement and RI-093, User Agreement.

## TERMS AND DEFINITIONS

Criminal History Record (CHR)

A CHR from LEIN is nonpublic records entered by the MSP, Criminal Justice Information Center and contains information on a person’s criminal history.

Criminal History Record Information (CHRI)

A CHRI from LEIN is background information obtained from the criminal history record.

Criminal Justice Agency (CJA)

An agency is considered a CJA if it is either a court, governmental agency, or any subunit of a governmental agency that performs administrative activities of criminal justice pursuant to a statute or executive order and allocates a substantial part of its annual budget to the administration of criminal justice.

Criminal Justice Information (CJI)

Criminal Justice Information is data (electronic or hard copy) collected by criminal justice agencies for the purposes as authorized or required by law. (Michigan Administrative Rule, R 28.5101(g)).

Law Enforcement Information Network (LEIN)

LEIN is Michigan's statewide-computerized information system that stores and disseminates criminal justice information (CJI).

Michigan Criminal Justice Information Network (MiCJIN)

MiCJIN is a portal or software bundle providing direct connection to the LEIN.

National Crime Information Center (NCIC)/III

The NCIC is a nationwide, computerized information system that helps the criminal justice community perform its duties by providing accurate and timely documented criminal justice information (for example, wanted person files, article files, missing person files).

The III is a cooperative state-federal system for the electronic exchange of criminal history record information for authorized purposes as specified by local, state, and federal laws.

Noncriminal Justice Agency (NCJA)

A NCJA that has access to CJI is any court, governmental agency, or any subunit of a government agency that performs administrative activities other than the administration of criminal justice.

Originating Agency Identifier (ORI)

The MSP provides an Originating Agency Identifier (ORI), as authorized by contractual agreement, to a governmental agency or

subunit defined as either a CJA or NCJA. The ORI separately identifies each unit/agency and each transaction made from that unit/agency must include the assigned ORI.

Person Query

A person query is a way to look up criminal justice information available in LEIN without using the criminal history record form. Queried information requires the same privacy and protections outlined herein this policy and the Criminal Justice Information Systems (CJIS) Security policy. Only perform a person query using the MiCJIN Talon Person Query, form.

Verified Information

Information obtained from credible public sources that corroborate information obtained from LEIN.

The following are credible sources to verify information:

- Courts.
- Internet Criminal History Tool (ICHAT).
- National and State sex offender registries.
- Offender Tracking Information System (OTIS).
- Police/law enforcement.
- Prosecuting attorney's office.
- Secretary of State (SOS).
- Self-disclosure.
- VINELINK.

## ROLES AND RESPONSIBILITIES

Each agency or sub-unit that has an assigned ORI(s) must appoint selected staff to serve as one or more of the following role(s): operator, terminal agency coordinator (TAC) and local agency security officer (LASO). An appointed person can serve dual roles as long they uphold all security policy and contract requirements.

Authorized User

An authorized user is an individual/group of individuals authorized to access CJI from LEIN as required by policy and as permitted access by law.

MDHHS authorized users typically include local county staff, such as an appointed requester, operator or terminal agency coordinator (TAC); services worker, office supervisor; manager; and director.

Central Office Local Agency Security Officer (LASO)

The central office LASO serves as the compliance expert for local county appointed LASOs. The LASO helps to ensure physical security, software compliance, and physical security screening requirements are adhered and immediately reports breaches to the MSP LEIN field services.

The LASO must:

- Identify who is using the approved hardware, software, and firmware and ensure that only authorized individuals have access.
- Ensure the upholding of personnel security-screening procedures, as outlined in this policy.
- Assist county LASO's to help ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and promptly inform the CJIS System Agency (CSA) information security officer (ISO) of security incidents.

Central Office Terminal Agency Coordinator (TAC)

The central office TAC is responsible for ensuring LEIN use compliance for MDHHS/CSA assigned ORI(s).

TAC's role/responsibility includes:

- Serve as a liaison to local county users and helps with supervision and system integrity across all assigned ORIs within the agency.
- Enable and disable TACs and operators.
- Monitor and track user compliance.
- Affirm and validate users in MiCJIN.

- Report any agency violations to MSP.
- Disseminate delay-hit notifications.
- Serve as the agency liaison between MSP and MDHHS for audit, contractual, training assistance and policy compliance.

For specific roles and responsibilities; see MSP TAC Manual.

Local Agency Security Officer (LASO)

A LASO serves as the county-appointed security contact for CJIS related issues. The LASO ensures physical security, software compliance, and physical security screening requirements are adhered and immediately reports breaches to the central office LASO.

The LASO must:

- Identify who is using the approved hardware, software, and firmware and ensure that only authorized individuals have access.
- Ensure the upholding of personnel security-screening procedures, as outlined in this policy.
- Ensure the approved and appropriate security measures are in place and working as expected.
- Support policy compliance and promptly inform the central office LASO of security incidents.

Operator

An operator receives and processes the necessary criminal history request forms provided by an authorized user under the assigned ORI and records and retains the transactions for audits. The Operator is responsible for ensuring safety and security of the generated criminal history information. For specific roles and responsibilities; see MSP Operations Manual.

Requester

A requester granted permission by policy and law requests criminal history record information from the local county operator or TAC.

Authorized requesters include services workers assigned to case files in the following units: Adoption, Adult Protective Services (APS), Children's Protective Services (CPS), Foster Care (FC), Adoption and Foster care Interstate Compact on the Placement of Children (ICPC) Juvenile Guardianship and Juvenile Justice (JJ).

The requester must be associated to the open/active case requiring the criminal history record information. The requester is knowledgeable in the policies that require a criminal history background check; see SRM 700, LEIN. The requester is responsible for interpreting and securing the criminal history report.

### Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact to the central office TAC and the local county authorized users. The TAC is responsible for LEIN use compliance for his/her county assigned originating agency identifier (ORI). TACs are trained by MSP. MSP-trained TACs are responsible for training county operators. For specific roles and responsibilities; see MSP TAC Manual.

## LEIN ACCESS

Local child welfare program offices have access to information in the Law Enforcement Information Network (LEIN) through a department agreement with the Michigan State Police. This access includes the following information:

- State of Michigan criminal history information.
- Sex Offender Registry.
- Missing/wanted persons.
- Prison and parole information.
- Gun registration/permits.
- Personal protection orders.
- Officer cautions.
- Michigan Secretary of State (SOS).
- National Crime Information Center (NCIC) - wants/warrants only within the United States (US).

**Note:** Full access may be restricted according to agency authorization. Criminal history information from outside the U.S. is restricted to criminal justice agencies.

Requirements for requesting LEIN; see SRM 700, Required LEIN Requests.

NCIC/III

The National Crime Information Center (NCIC) contains restricted and non-restricted interface files. The NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use; see, CJIS Security Policy v5_5 §4.2. Proper access and dissemination of data from the restricted files must be consistent with the access and dissemination policies for the III as described in 28 CFR Part 20 and the NCIC Operating Manual.

34 USC 20961 authorizes state access to NCIC/III files for purposes of obtaining national criminal history information on persons involved in cases of child abuse, neglect or exploitation.

ACCESS CONTROL

Name-based background checks through LEIN/NCIC III are required before granting any access to CJI.

The FBI recommends that agencies perform follow up name-based background checks at least once every five years to ensure that an employee has not had a disqualifying arrest/conviction and not told the employer. If RAPBACK is available, then this follow up recommendation or requirement is not necessary after submitting to the initial fingerprint clearance.

Direct Access

The MDHHS, Children's Services Administration (CSA) is a direct access agency with access to non-public LEIN information via the MiCJIN. A person who directly accesses nonpublic LEIN information is the appointed Operator(s) and TAC(s).

Obtaining authorization for direct access to CJI a person must complete the following:

- Pass a state and federal fingerprint criminal history background check.
- Attend an operator and/or TAC training. Have a passing grade of no less than 70 percent.
- Attend a LEIN security awareness training.

- Sign forms: MDHHS 5518, LEIN Notice of Criminal Penalties, and MDHHS 5528, Access & Operator Request: Security Agreement.

To remain an Operator and/or TAC update all training and forms once every two years.

To maintain system integrity and reduce the threat for potential breach, appointed positions are limited. The allowable number of operators per county is a ratio of .15 percent of the number of total requesters at that location. For example, a county with 40 requesters can have up to six operators (40 x .15=6). The allowable number of TACs per county is one primary with two serving as back up. To request additional operators and/or TACs beyond the noted ratio send a justification request to the central office TAC.

***Fingerprint Clearance Application***

For an applicant to apply for a fingerprint clearance for direct access to LEIN, complete the following process:

1. Complete form RI-030, LiveScan Fingerprint Background Check Request. This form is required by MSP to verify staff authorized permission to be fingerprinted allowing MDHHS to receive the individuals criminal history record.

2. Schedule a fingerprint appointment or go to a police station. Have the representative conducting the fingerprinting sign the RI-030.

3. Submit signed RI-030 to the TAC to retain for audit purposes.

Fingerprint results for LEIN access are criminal history records that require the same confidentiality as LEIN reports.

Indirect Access

Indirect access is having the authority to review CJI; but, without direct access to MiCJIN, as used to conduct transactional activity within the LEIN.

Authorized users with indirect access may include any agency staff who requires to review and interpret CHRI as part of case review. Staff may include, but is not limited to requesters, supervisors, managers and directors.

Authorized users who review LEIN criminal history report information (CHRI) must sign the MDHHS 5518, LEIN Notice of Criminal Penalties, form and take the LEIN security awareness training within the first six months of hire and again once every two years thereafter.

### Access Validation

Local office TAC must annually review all account access and report the validation to the central office TAC.

TAC or LASO must annually review authorized user access to ensure that access and account privileges commensurate with the following statuses/need: job functions, policy requirements, and employment status on systems that contain CJI. Immediately report to the central office TAC any changes to the status of either an operator or TAC:

- Any extended leave of more than 30 days.
- Termination or departure.
- Any name changes.
- Any transfer to another county office.
- Not accessing their account in 6 months.
- Any violations of use of CJI.
- Any other need for direct access removal.
- Any violations or misuse.

Penalties for violating this policy section may result in network removal, access revocation, or corrective or disciplinary action, and termination of employment.

## PHYSICAL PROTECTION REQUIREMENTS

To access and view CJI from LEIN, secure the physical location according to the below MSP-approved layout as described in this policy, and in accordance to the CJIS security policy.

### Physically Secure Location

A physically secure location is a facility, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the LEIN-based CJI and associated information systems. The perimeter of the physically

secure location should be noticeably identifiable and separated from non-secure locations by physical controls. Define the security perimeters as controlled and secured. Identify the restricted non-public areas with a sign at the entrance.

To meet the physical protection requirements, units and counties with access to CJI must create a secured area with either a preferred set up or a controlled area.

***Preferred Set Up***

The preferred secure room set up is to have one vacant room with the following: a lock-capable door, a posted sign on the door that reads “Processing CJI…Do Not Enter”, and shared printers must have lock/password capability. This room can have multiple computers that are only accessible by the local county LEIN operator(s) and terminal agency coordinator(s) (TACs).

***Controlled Area***

Controlled areas are configured working stations assigned to operators for purposes of processing CHRI requests from LEIN. Configured LEIN operator stations shall include the following:

- May have up to five cubicle configurations in the county office, depending on the number of operators per county.
- Position monitors used to query/view CJI away from door or entry of cubicle.
- Place privacy screen filters on monitors even when monitors are not facing the cubicle opening to restrict viewing by unauthorized personnel who may enter cubical.
- Ensure cubicle walls are high enough to restrict viewing by the average height person.
- Lock up any physical media such as LEIN printouts, TAC Manual, LEIN Manual, Etc. when not in use.
- Power off computers after working hours.
- Use the windows system lock during working hours when employees are away from their desk.
- Only have the LEIN application open when performing LEIN queries.

- Create a sign to place on the outside of cubical when processing CJI. Example: “Processing CJI…do not enter”

- If printing CJI on a shared printer, use the lock job function so the CJI does not print until the authorized person at the printer.

For counties with multiple floors/areas with open cubicles that access CJI from LEIN, ensure that the doors that access the multiple rooms where CJI is accessed is locked and any unescorted access to those rooms complete level 1 security awareness requirement by signing the MDHHS-5502, Security Awareness Acknowledgement for Personnel with Only Physical Access to Physically Secure Locations, form.

**Note:** Controlled areas may include cubicles or other vacant office spaces based on county capacity. Cubicle configuration design for LEIN operators is on file with the Bureau of Organizational Services. Directors are to contact the central office TAC to discuss variations of office arrangement that will meet compliance.

**Note:** Configured cubicles will become the permanent operator station. When the appointed operator is no longer serving his/her role and another staff is appointed, the worker must vacate the station for the new operator to assume.

## PHYSICAL ACCESS AUTHORIZATIONS

Authorized users must take the necessary steps to prevent and protect the agency from physical, logical and electronic breaches. They are responsible for maintaining a current list of authorized users and informing the central office TAC of any changes.

All users with physical access must meet the following requirements:

- Meet the minimum personnel screening requirements prior to CJI access.

  - Conduct a state and federal fingerprint-based record check within 30 days of assignment for all LEIN users who have **direct** access to CJI.

  - Complete and sign the DHHS-5518, Notice of Criminal Penalties, form and LEIN Security Awareness Training certificate within six months of hire and recertify once every two years thereafter.

- Be aware of who is in their secure area before accessing confidential data.
  - Take appropriate action to protect all confidential data.
  - Protect all terminal monitors with viewable CJI displayed on monitor and not allow viewing by the public or escorted visitors.
  - Private contractors/vendors and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be escorted or required to sign the MDHHS-5502, Security Awareness. Acknowledgment for Personnel with Only Physical Access to Physically Secure Locations, form.
- Protect and not share any individually issued keys, proximity cards, computer account passwords, etc.
  - Report loss of issued keys, proximity cards, etc.
  - Safeguard and not share passwords, personal identification numbers (PIN), security tokens (such as VPN), and all other facility and computer systems security access procedures.
- Protect computer/tablet from viruses, worms, Trojan horses, and other malicious code; see APL 68E-110, Protection from Malicious Software Policy and Procedure.
- Protect web usage; see Information Technology Support: DTMB/IT in this item.
- Do not use personally owned devices on the computers with CJI access.
- Secure dissemination and review of CHRI when sending or receiving via phone, fax or email. Follow physical access authorization requirements detailed within this policy.
- Report any physical security incidents to the central office TAC and LASO to include facility access violations, loss of CJI, and loss of laptops, cellular phones, thumb drives, CDs/DVDs and printouts containing CJI.
- Properly release CJI only to authorized personnel and crosscut shredded printouts when no longer needed.

- Ensure data centers with CJI are physically and logically secure.
- Keep the TAC informed of when CJI access is no longer required. In the event of terminated employment, the individual must surrender all property and access managed by MDHHS and DTMB.
- Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter unprotected, such as door propped opened.

Authorized Unescorted Access

Personnel with access to physically secure locations or controlled areas, but do not directly or indirectly access CJI must take level one security awareness training. These personnel include, but are not limited to: support personnel, other MDHHS unit staff, private contractors/vendors and custodial workers.

Level one security awareness access includes reviewing and signing the MDHHS-5502, Security Awareness Acknowledgment for Personnel with Only Physical Access to Physically Secure Locations. Completion of this form is required before granting authorization for unescorted access to secure areas.

Authorized Escorted Access

An escort is an authorized user who always accompanies a visitor while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

A visitor is a person who visits the MDHHS facility on a temporary basis, who is not a MDHHS employee and who requires escorted access to the physically secure locations within the MDHHS where LEIN-based CJI and associated information systems.

Visitors must:

- Check in before entering a physically secure location.
- Be accompanied by a MDHHS authorized user as an escort at all times.

- Follow the MDHHS policy for authorized unescorted access:
  - For personnel who require frequent unescorted access to restricted area(s).
  - For private contractors/vendors who requires frequent unescorted access to restricted area(s).
- Not be allowed to view screen information mitigating shoulder surfing.
- Not be allowed to sponsor another visitor.
- Not enter into a secure area with electronic devices unless approved by the MDHHS LASO to include cameras and mobile devices. No photographs allowed without permission of the MDHHS assigned personnel.

Courteously escort individuals not having any legitimate business in the restricted area to a public area of the facility. Workers should question any unescorted stranger in a physically secure area. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

Authorized Offsite Access

Authorized offsite access is when a MDHHS authorized users, accessing CJI from LEIN has been given authorization to directly access the MiCJIN portal from outside of the worker's assigned home agency office building.

Having authorized offsite access requires the operator to access either from his /her personal home or from a non-assigned local county MDHHS office. A worker must not access the MiCJIN portal using a public connection for example, a coffee shop, at a client's residence, using hotspot, etc.

Requirements for direct access from personal home must:

- Adhere to the CJIS security policy on physical security requirements.
- Allow for the possibility of in-home audits.
- Only connect to internet via either an ethernet cord or Wi-Fi.

- Only use the agency-issued computer.
- Always connect to VPN before logging into MiCJIN.
- Not print LEIN results from a home printer, (if needed to view again, it is best to simply re-run).
- Not store CHRI on a network drive unless it is restricted, monitored and tracked by a local county TAC for appropriate authorized access.

Requirements for accessing from a non-assigned local county MDHHS office:

- Adhere to CJIS security policy on physical security.
- Connect directly to state of Michigan Wi-Fi or direct ethernet.
- Ensure connection to MDHHS system or if Wi-Fi, must connect to VPN before logging into MiCJIN.

Penalties

Violation of any of the requirements in this policy by any authorized user will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

INFORMATION TECHNOLOGY SUPPORT: DTMB/IT

In coordination with above roles, all MSP-vetted DTMB IT support staff will protect CJI from compromise at the MDHHS by adhering to the MDHHS/DTMB Management Control Agreement (MCA) and the DTMB policies found at the Michigan Department of Technology, Management and Budget website under Technology/IT Policies, Standards & Procedures (PSP); in particular see Policy 1370, Information Technology Configuration Management.

## PROCESS FOR REQUESTING A LEIN RECORD

CJI can only be requested by MDHHS requesters who are assigned to the active case and requested for purposes outlined in policy. The person's name as reflected in the case file should be the name written on the DHS-268 and DHS-269 forms.

After the request, the operator must complete the DHS-268 Clearance Log, and an authorized user must sign it upon picking up the LEIN CHRI.

These forms must also include the associated case number, investigative or intake ID number.

## PROCESS FOR REQUESTING DIRECT ACCESS

Only TACs and operators can have direct access to MiCJIN/LEIN. To appoint a TAC or operator, first a schedule appointment to be state and national fingerprinted using the RI-030, LiveScan Fingerprint Background Check Request, form.

Upon notification of fingerprint clearance, the following steps can then occur:

1. Attend required TAC and/or operator training.
2. Take a test with a passing grade of no less than 70 percent.
3. Review the LEIN security awareness training and sign the certificate.
4. Sign both forms: 5518, LEIN Notice of Criminal Penalties, and 5528, Access & Operator Request: Security Agreement.
5. Turn all tests and documents into the local county TAC to compile.

The local county TAC will bundle the information and forward copies to the central office TAC. The originals will remain on file at the county office. See Record Retention and Disposal Schedule, 49/BCWF, Child Welfare Policy and Programs for record retention policy.

Select Child Welfare Policy and Programs 49BCWF. If the web link does not work please call 517-335-9132 if you need a copy of an agency-specific schedule

Renew the tests and forms once every two years to continue to serve in the appointed role.

## DISSEMINATION AUTHORITY

No information solely from LEIN shall be included in department reports, including any electronic case records. Workers must verify LEIN information by public source(s), which then can be cited. See SRM, 700, LEIN for requirements for documenting in reports, files or narratives and dissemination authority.

## VIOLATIONS AND BREACHES

CJIS Policy Council Act, MCL 28.214(6)(a) explains penalties to a person who intentionally uses or discloses nonpublic information for personal gain or in a manner that is not authorized by law or rule.

The first offense is a misdemeanor punishable by 93 days imprisonment or $500 fine, or both. The second offense is a felony punishable by not more than four years imprisonment or $2,000 fine, or both.

Staff found to have misused LEIN information will be subject to disciplinary action up to and including dismissal.

### Incident Response

Immediately report all suspected violations of LEIN policy pertaining to unauthorized access, use or disclosure to the local office TAC and the central office TAC.

The central office TAC must report the incident to MSP LEIN field services with a copy to the Office of Inspector General (OIG). MSP will conduct investigation and may send a letter for agency investigation and either with a request for corrective action plan or with penalty recommendations.

## FORMAL AUDITS

Local office TACs are responsible for periodically validating LEIN use to ensure proper use and procedures of accessing LEIN information. The MSP will triennially audit county use.

## POLICY CONTACT

For questions about this policy contact Joy Thelen, central office TAC at the CPS Program Office via email at ThelenJ12@michigan.gov